TRANSFER OF SECURITY DATA BETWEEN TWO MEMORIES

TECHNICAL FIELD OF THE INVENTION

The present invention relates to the field of safe transfer of security data from one memory to another in an electronic data processing environment. In particular the present invention relates to a method of transferring data from a non-volatile memory to a working memory of an electronic data processing device, such an electronic data processing device as well as to a device for blocking write attempts.

DESCRIPTION OF RELATED ART

The cellular phones of today have more and more different functions and applications in them. One such function is the possibility to make economical transactions. In performing transactions there is normally used security data in the form of private encryption keys. The storage of these keys has to be safe and safeguarded from manipulation.

In relation to cellular phones these keys have up till now been stored in so-called NOR flash memories. These known memories are of the type XIP (execute in place), which means that the keys are not moved from the memory. It is today possible to block writing of the position of such keys on such a memory using hardware solutions. Such solutions monitor program execution and data access on the system bus inside the phone. Software code that is not part of the authenticated firmware of the device is prevented from accessing the keys. These solutions assume that at least the firmware and possibly the keys are located in an XIP memory, so that address patterns on the bus are fixed for any given execution sequence.

Such NOR flash memories are however relatively expensive, why there is a trend to replace them with so-called NAND flash memories, which are cheaper. These memories are however not of the XIP type, and in order to use the content stored on them, the content has to be moved or copied to a working memory of the phone.

There is therefore a need for being able to protect such security data from manipulation when it is being moved from the NAND flash memory to the working memory.

It is furthermore often desirable to provide such a protection independently of the central processing of the unit, since otherwise other units such as a debugging unit, which is often a part of the phone for development reasons, can influence such security information.

SUMMARY OF THE INVENTION

The present invention is thus directed towards solving the problem of protecting the security data from manipulation, when it is moved from a non-volatile memory to a working memory as well as after such relocation.

This is achieved by copying data from the non-volatile memory to the working memory, which data includes security data to be write-protected, activating blocking of the security data in the working memory, monitoring all communication with the working memory, and blocking all write attempts to the copied security data stored in the working memory, where activating blocking, monitoring communication and blocking write attempts are performed independently of the central processing unit of the data processing device, such that the central processing unit cannot manipulate the security data.

One object of the present invention is to provide a method that protects security data from manipulation when the data is moved from a non-volatile memory to a working memory as well as after such relocation.

According to a first aspect of the present invention, the object is achieved by a method of transferring data from a non-volatile memory to a working memory of an electronic data processing device, comprising the steps of:

copying data from the non-volatile memory to the working memory, which data includes security data to be write-protected,

activating a blocking of the security data in the working memory,

monitoring all communication with the working memory, and

blocking all write attempts to the copied security data stored in the working memory,

wherein at least the steps of activating a blocking, monitoring communication and blocking write attempts are performed independently of the central processing unit of the data processing device, such that the central processing unit cannot manipulate the security data.

A second aspect of the present invention is directed to a method including the features of the first aspect, wherein the area of the security data in the non-volatile memory is pre-defined and pre-stored in a device for blocking write attempts and used at least in relation to activating a blocking.

A third aspect of the present invention is directed towards a method including the features of the first aspect, wherein the step of copying data comprises copying only the security

data from the non-volatile memory to the working memory independently of the central processing unit of the data processing device and copying any further data under the control of the central processing unit of the device.

A fourth aspect of the present invention is directed towards a method including the features of the third aspect, wherein the area of the security data in the non-volatile memory and the area for storage of the security data in the working memory are pre-defined and wherein the step of activating a blocking of positions of the working memory is triggered by the copying being made to the pre-defined area in the working memory and the blocking is activated for said area.

A fifth aspect of the present invention is directed towards a method including the features of the first aspect, wherein the step of copying comprises copying all data from the non-volatile memory to the working memory under the control of the central processing unit of the device.

A sixth aspect of the present invention is directed towards a method including the features of the fifth aspect, wherein the area of the security data in the non-volatile memory is pre-defined and wherein the step of activating a blocking is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area of the working memory and the blocking is activated for that area of the working memory.

A seventh aspect of the present invention is directed towards a method including the features of the first aspect, wherein the step of blocking is achieved by changing the destination address of the data transferred to the working memory.

An eighth aspect of the present invention is directed towards a method including the features of the first aspect, further comprising the steps of disconnecting a debugging unit at least when copying the security data to the working memory and reconnecting the debugging unit when the blocking has been activated.

Another object of the present invention is to provide a device for blocking write attempts to security data that protects security data from manipulation when the data is moved from a non-volatile memory to a working memory as well as after such relocation.

According to a ninth aspect of the present invention, this object is achieved by a device for blocking write attempts to security data transferred from a non-volatile memory to a working memory in an electronic data processing environment that includes a central processing unit and comprising:

a monitoring unit arranged to:
activate a blocking of the security data in the working memory upon copying of the security data from the non-volatile memory to the working memory,
monitor all communication with the working memory, and
block all write attempts to the copied security data stored in the working memory,
all performed independently of the central processing unit of the data processing environment, such that the central processing unit cannot manipulate the security data.

A tenth aspect of the present invention is directed towards a method including the features of the ninth aspect, wherein the area of the security data in the non-volatile memory is pre-defined and pre-stored in the device and used in relation at least to activating a blocking.

An eleventh aspect of the present invention is directed towards a device including the features of the ninth aspect, further comprising a copy control unit arranged to copy the security data from the non-volatile memory to the working memory also independently of the central processing unit of the data processing environment.

A twelfth aspect of the present invention is directed towards a device including the features of the eleventh aspect, where the area of the security data in the non-volatile memory and the area for storage of the security data in the working memory are pre-defined and pre-stored in the device and the monitoring unit when activating a blocking is triggered by the copying being made to the pre-defined area in the working memory and activates a blocking of that area.

A thirteenth aspect of the present invention is directed towards a device including the features of the ninth aspect, where the area of the security data in the non-volatile memory is pre-defined and pre-stored in the device and the monitoring unit when activating a blocking is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area of the working memory and activating a blocking for that area of the working memory.

A fourteenth aspect of the present invention is directed towards a device including the features of the ninth aspect, wherein the monitoring unit is arranged to block write attempts by changing the destination address of data transferred to the working memory.

A fifteenth aspect of the present invention is directed towards a device including the features of the ninth aspect, wherein the monitoring unit is arranged to disconnect a debugging unit of the electronic data processing environment at least when the security data is copied to the working memory and to reconnect the debugging unit when the blocking has been activated.

A sixteenth aspect of the present invention is directed towards a device including the features of the ninth aspect, wherein it is implemented in hardware.

Yet another object is to provide an electronic data processing device that protects security data from manipulation when the data is moved from a non-volatile memory to a working memory as well as after such relocation.

According to a seventeenth aspect of the present invention, this object is achieved by an electronic data processing device comprising:

a non-volatile memory comprising data including security data to be write-protected,

a working memory,

a central processing unit arranged to control copying of at least some data from the non-volatile memory to the working memory, and

a device for blocking write attempts to security data transferred from the non-volatile memory to the working memory and comprising a monitoring unit arranged to:

activate a blocking of the security data in the working memory upon copying of the security data from the non-volatile memory to the working memory,

monitor all communication with the working memory, and

block all write attempts to the copied security data stored in the working memory,

all performed independently of the central processing unit, such that the central processing unit cannot manipulate the security data.

An eighteenth aspect of the present invention is directed towards a device including the features of the seventeenth aspect, wherein the area of the security data in the non-volatile memory is pre-defined and pre-stored in the device for blocking write attempts and used in relation at least to activating a blocking.

A nineteenth aspect of the present invention is directed towards a device including the features of the seventeenth aspect, wherein the device for blocking write attempts further

comprises a copy control unit arranged to copy the security data from the non-volatile memory to the working memory independently of the central processing unit and the central processing unit is arranged to control the copying of further data from the non-volatile memory to the working memory.

A twentieth aspect of the present invention is directed towards a device including the features of the nineteenth aspect, where the area of the security data in the non-volatile memory and the area for storage of the security data in the working memory are pre-defined and pre-stored in the device for blocking write attempts and the monitoring unit when activating a blocking is triggered by the copying being made to the pre-defined area in the working memory and activates a blocking of that area.

A twenty-first aspect of the present invention is directed towards a device including the features of the seventeenth aspect, wherein the central processing unit is arranged to control the copying of all data from the non-volatile memory to the working memory.

A twenty-second aspect of the present invention is directed towards a device including the features of the twenty-first aspect, where the area of the security data in the non-volatile memory is pre-defined and pre-stored in the device for blocking write attempts and the monitoring unit when activating a blocking is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area of the working memory and activating a blocking for that area of the working memory.

A twenty-third aspect of the present invention is directed towards a device including the features of the seventeenth aspect, wherein the monitoring unit is arranged to block write attempts by changing the destination address of data transferred to the working memory.

A twenty-fourth aspect of the present invention is directed towards a device including the features of the seventeenth aspect, further comprising a debugging unit and wherein the monitoring unit is arranged to disconnect the debugging unit at least when the security data is copied to the working memory and to reconnect the debugging unit when the blocking has been activated.

A twenty-fifth aspect of the present invention is directed towards a device including the features of the seventeenth aspect, wherein the device for blocking write attempts is implemented in hardware.

A twenty-sixth aspect of the present invention is directed towards a device including the features of the seventeenth aspect, wherein the device is a portable communication device.

A twenty-seventh aspect of the present invention is directed towards a device including the features of the twenty-sixth aspect, wherein the device is a cellular phone.

The invention has the following advantages. It enables the storage of security data in a working memory without risking tampering of this data, which is guaranteed by the independence from the central processing unit. Another advantage is that cheaper memories therefore can be used instead of the memories that would otherwise be needed. It also allows the possibility to keep a debugging unit in the electronic data processing device for debugging software loaded in the device without having to compromise the safety of the security data.

It should be emphasized that the term "comprises/comprising" when used in this specification is taken to specify the presence of stated features, integers, steps or components, but does not preclude the presence or addition of one or more other features, integers, steps, components or groups thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described in more detail in relation to the enclosed drawings, in which:

fig. 1 shows a block schematic of an electronic processing device including a device for blocking write attempts both according to a first embodiment of the invention,
fig. 2 shows a flow chart of a method according to the first embodiment of the invention,
fig. 3 shows a block schematic of an electronic processing device including a device for blocking write attempts both according to a second embodiment of the invention, and
fig. 4 shows a flow chart of a method according to the second embodiment of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS

An electronic data processing device 10 according to a first embodiment of the invention is shown in a block schematic in fig. 1. The device is preferably provided in a portable communication device and in the preferred embodiment the device is provided in a cellular phone and then a so-called smartphone. A cellular phone is just one example of where the

invention can be implemented. The invention can for instance also be used in a PDA (personal digital assistant), a palm top computer, a lap top computer and in a PC (personal Computer). The device where the electronic data processing device according to the invention is implemented should however have functionality for secure transferring and transactions.

The device 10 includes a communication bus 12 to which are connected a central processing unit 14, a device for blocking write attempts 16, a ROM memory 18 and an interface 20 towards external memories. The device 16 includes a monitoring unit 28, the functioning of which will be described in more detail layer. To the interface 20 are connected a working memory 22, which preferably is a volatile so-called SD RAM memory and a non-volatile NAND flash memory 24. A debugging unit 26 is also connected to the bus 12. The NAND flash memory includes an area defined by memory addresses A1 and A2, which area comprises security data 30 in the form of private cryptographic keys. The working memory 22 includes a corresponding area defined by memory addresses B1 and B2, which is to receive the private security keys.

The main functioning of the electronic data processing device is, as is well known to the man skilled in the art, to execute software stored in different memories under the control of the central processing unit. Some such software can be some type of transactions software originally stored in the NAND flash memory. The information on a NAND flash memory cannot be used directly, but this information has to be transferred to a working memory before being used. If this is done in a straight-forward way, without taking necessary precautions, this data can be tampered with, which is highly undesirable if the data includes private keys to be used in for instance transactions involving money. One such source of tampering can be the debugging unit, which is connected to the device in order to debug faulty programs. This debugging unit often has contact with other devices, like computers and servers and can take control of the central processing unit of the electronic processing device and is therefore a potential safety risk for the data that is transferred.

The device and method according to a first embodiment of the invention takes care of some of these safety aspects. Therefore the performance of the device according to this first embodiment will now be explained with reference being made to fig. 2, which shows a flow chart of a method according to this first embodiment of the invention.

At start-up of the device 10 the data in the flash memory 24 has to be transferred to the working memory 22, which in this first embodiment is done under the control of the central processing unit 14. Before this is done, the monitoring unit 28 in device for

blocking write attempts 16 disconnects or turns off the debugging unit 26, step 32, in order to safeguard that the security keys in the flash memory 24 will not be tampered with after copying. This turning off is thus done independently from the central processing unit 14. Thereafter the monitoring unit 28 monitors the traffic on the bus 12, step 34. Traffic on the bus is sent using source and destination addresses. As mentioned before the copying of data is performed under the control of the central processing unit 14, step 36. This unit 14 therefore controls the ROM memory 18, which includes transferral codes for transferring all the data in the flash memory 24 to the working memory 22. Here the data from the flash memory 24 can be stored in any position in the working memory 22. The content of the flash memory 24 is transferred sequentially. The monitoring unit 28 is set to look out for the memory addresses A1 and A2 defining the area of the security keys 30 in the flash memory on the data bus 12. This information is pre-set and pre-stored in the monitoring unit 28 and therefore provided beforehand in the monitoring unit 28. When the first of the information is transferred from address A1 to address B1 in the working memory, the monitoring unit begins activating blocking through storing the destination address B1. It then waits until the last address A2 of the area is transferred to destination address B2, which it also stores. The monitoring unit then locks the data area B1 – B2 of the working memory 22, since then the keys 30 have been copied. In this way blocking of the address area defined by addresses B1 and B2 was activated by the monitoring unit upon the first detection of data transfer from the area defined by addresses A1 and A2, step 38. The monitoring unit then reconnects or turns on the debugging unit 26, step 40, so that it can function yet again. After this the monitoring unit 28 continues monitoring all the traffic on the bus, step 42, and blocks all attempts to write to the area defined by addresses B1 and B2, step 44. This blocking is normally done through controlling the interface 20 to change address whenever a write command to any address in the area is encountered. Steps 38 – 44 are all performed by the monitoring unit independently of the central processing unit 14. The device 16 including the monitoring unit 28 is provided in the form of hardware in the form of suitably selected and connected logic circuits. This makes the device 16 work fast. Another advantage is that the functioning of it cannot be changed, which makes illegal tampering of the device hard, so that write-protection of the moved security keys can be guaranteed.

Now a second embodiment of the invention will be described with reference being made to fig. 3 and 4. Fig. 3 shows a device 10 that is similar to the device in fig. 1. There is only one difference here and that is that the device for blocking write attempts 16 also includes a copy control unit 46. This unit 46, which in this embodiment is a DMA (Direct Memory Access) unit, takes care of the transfer of the keys in the area A1 – A2 in the flash memory 24 to the area B1 – B2 of the working memory 22. As in the first embodiment, the monitoring unit 28 in device 16 here disconnects or turns off the debugging unit 26, step

48, in order to safeguard that the private security keys 30 in the flash memory 24 will not be tampered with after copying. Thereafter the copy control unit 46 copies the keys 30 in the area defined by addresses A1 and A2 in the flash memory 24 to the area defined by addresses B1 and B2 in the working memory 22, step 50. In this case both the addresses A1 – A2 and addresses B1 – B2 are pre-defined and pre-stored in the copy control unit 46 and therefore provided beforehand. The copy control unit 46 here also transfer this content sequentially. When the copy control unit 46 has copied these addresses it notifies the monitoring unit 28, which then goes on and activates blocking of the area defined by addresses B1 and B2, step 52. The monitoring unit 28 can also have these addresses B1 and B2 pre-stored or receive them from the copy control unit 46 upon signalling of finished copying. The monitoring unit 28 then reconnects or turns on the debugging unit 26, step 54, so that it can function yet again. Thereafter the monitoring unit 28 starts monitoring all the traffic on the data bus, step 56. The central processing unit 14 transfers the rest of the content from the flash memory 24 to the working memory 22, step 58, which is done in the same way as was described in relation to the first embodiment. The monitoring unit 28 then blocks all attempts to write to the area defined by addresses B1 and B2, step 60. This blocking is done in the same way as was described in the first embodiment. Steps 48 – 56 and 60 are all performed by the monitoring unit independently of the central processing unit. The device for blocking write attempts 16 including the copy control unit 46 and the monitoring unit 28 is also here provided in the form of hardware for making illegal tampering of the device hard, so that write-protection of the moved security keys can be guaranteed.

When the electronic data processing device is turned off, the working memory is emptied, which means that the data in the flash memory has to be transferred each time the device is turned on again or rebooted.

The present invention has many advantages. It enables the storage of the private security keys in a working memory without risking tampering of these keys, which is guaranteed by the independence of the central processing units. Another advantage is that cheaper memories therefore can be used instead of the memories that would otherwise be needed. It also allows the possibility to keep a debugging unit in the device for debugging software loaded in the device without having to compromise the safety of the security keys.

The present invention can be varied in many ways. The different method steps do not necessarily all have to be provided in the order described. It is however essential that the debugging unit is turned off before the keys are transferred and that the activating of a blocking or locking follows immediately after the transfer of the keys. The flash memory can be included in the device or be an external memory that is connected to the device. It

can also include other data than the keys and any software associated with the keys. The working memory can of course also include other types of information. It is possible that the flash memory, in the first described embodiment can have the addresses of the defined area in the working memory stored at a specific location, which location the ROM memory then can access for finding out the destination address of the security keys. The invention is furthermore not limited to private security keys, but can be applied on any data that needs to be write-protected. In view of this the present invention is therefore only to be limited by the following claims.